

**OCC Quarterly Report on Year 2000 Activities**  
**Submitted to Congress September 4, 1998**

**AGENCY PROGRESS**

- 1. Following the same OMB reporting format as last quarter, please provide an updated progress report on the status of internal agency Year 2000 efforts. Please highlight any significant changes, especially schedule slippages, from last quarter in the status of mission critical systems. In the case of any slippages, please explain the cause of the slippages and actions instituted to correct the problem and get back on schedule.**

The OCC is aggressively converting our internal systems, and we expect to reach all of our established goals well before the Treasury Department deadlines. OCC managers in charge of internal Year 2000 efforts report weekly to the OCC's Year 2000 Oversight Committee to discuss progress and pending issues.

*Cost.* Through the second quarter of 1998, the OCC has expended \$3,658,000 on Year 2000 *internal* renovation, and we expect to spend an additional \$4,290,000 to complete this effort for a total expected outlay of \$7,948,000. Table 1.1 provides a summary of internal Year 2000 expenses. While our previous Quarterly Report showed total *internal* expenditures of \$10,804,000 for the 1996-2000 time period, this report shows \$7,948,000 in *internal* expenditures during that time. The difference in these figures -- approximately \$2,800,000 -- represents a change in our accounting for Year 2000 expenses. We decided to attribute certain training and contractor costs previously included in our cost estimate for *internal* remediation to our *external* Year 2000 program.

<b>Table 1.1</b>		
<b>OCC Year 2000 <i>Internal</i> Expenses *</b>		
Year	Y2K Renovation Expenditures	Estimated Cost to Completion
1996	\$ 15,000	--
1997	534,000	--
1998 - 1st 2 quarters	3,109,000	--
1998 - last 2 quarters	--	\$3,109,000
1999	--	1,072,000
2000	--	109,000
Subtotal	\$3,658,000	\$4,290,000
Total Internal Expenses	\$7,948,000	

\*Internal Expenses: Year 2000 personnel, contractor, training and software/code renovation costs associated with OCC internal IT systems. Also, personnel, contractor and miscellaneous costs for the assessment of OCC Non-IT systems. External Expenses: Personnel, contractor, training and other costs associated with OCC's assessment of the Year 2000 efforts of supervised financial institutions and independent data centers. Note: these expenditures do not include overhead expenses.

*Mission-Critical IT Systems.* The OCC identified 13 mission-critical information technology (IT) systems that support the key business functions of the agency.<sup>1</sup> One of the 13 will be retired (Trust Billing); the remaining 12 mission-critical IT systems have been assessed and will be repaired. Our original plan was to complete the renovation, validation, and implementation of all of our 12 mission-critical systems by July 31, 1998, well in advance of the Treasury Department's December 31, 1998, deadline. As of August 31, 1998, the OCC had renovated, validated as Year 2000 compliant, and implemented nine of the mission-critical IT systems. However, completion of the final three mission-critical IT systems is slightly behind our original plan.

As part of our internal renovation plan, we contracted with Information Analysis Incorporated (IAI) software factory on May 22, 1998. IAI agreed to complete renovation of portions of the three remaining mission-critical IT systems and six non-mission-critical IT systems. IAI experienced scheduling problems which delayed renovation, which in turn delayed OCC's original July 31, 1998, implementation date. All of the remaining three mission-critical IT systems have now been renovated. We expect to implement these systems in September and early October. Table 1.2 reviews the schedule for remediating the OCC's mission-critical IT systems.

<p align="center"><b>Table 1.2</b> <b>OCC Mission-Critical IT Systems Schedule</b></p>							
<b>System</b>	<b>Renovation</b>	<b>Validation</b>	<b>Implementation</b>	<b>IV&amp;V*</b>	<b>Certification</b>	<b>Contingency Plan</b>	<b>Trigger Date</b>
CAS	✓	✓	✓	10/31/98	11/7/98	✓	1/3/2000
TTRS	✓	✓	✓	10/31/98	11/7/98	✓	1/3/2000
TE	✓	✓	✓	10/31/98	11/7/98	✓	1/3/2000
SA	✓	✓	✓	9/30/98	10/7/98	✓	1/5/2000
GFS	✓	✓	✓	9/30/98	10/7/98	✓	1/3/2000
BA	✓	✓	✓	9/30/98	10/7/98	✓	1/31/2000
LOCKBOX	✓	✓	✓	9/30/98	10/7/98	✓	1/3/2000

---

<sup>1</sup> The mission-critical systems are Consolidated Application System (CAS), Time and Travel Reporting System (TTRS), Time Entry (TE), General Financial System (GFS), Salary Allocation (SA), Bank Assessment (BA), Lockbox, Security Authorization (AZ), Budget Code Restructure (BCR), Corporate Activities Information System (CAIS), Supervisory Monitoring System (SMS), National Bank Surveillance Video Display System (NBSVDS), and Trust Billing.

<p align="center"><b>Table 1.2</b> <b>OCC Mission-Critical IT Systems Schedule</b></p>							
AZ	✓	✓	✓	10/31/98	11/7/98	✓	6/1/1999
BCR	✓	✓	✓	8/31/98	9/8/98	✓	1/3/2000
CAIS	✓	10/10/98 ▲	10/18/98 ▲	10/15/98	10/22/98	✓	1/1/2000
SMS	✓	9/11/98 ▲	9/27/98 ▲	9/15/98	9/22/98	✓	1/1/2000
NBSVDS	✓	9/11/98 ▲	9/27/98 ▲	9/15/98	9/22/98	✓	1/1/2000
Trust Billing	■	■	■	N/A	N/A	N/A	N/A

\* **IV&V** - Independent Validation and Verification

■ Retiring system on or before 8/31/98. Not necessary to make Y2K compliant.

✓ Completed

▲ Dates extended due to request from IAI for extension to renovate software.

The OCC's mission-critical IT systems exchange data with five external parties: the Federal Reserve (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Finance Center (NFC), Treasury and the First National Bank of Chicago (FNBC). The OCC established bridge programs for data exchanges with the NFC and the FNBC. Of the OCC's 31 external data exchanges, 19 are Year 2000 compliant and 12 (FDIC - eight exchanges and FRB - four exchanges) are not Year 2000 compliant. The remaining 12 noncompliant data exchanges are awaiting testing before implementation. The OCC meets monthly with its primary data exchange partners to discuss compliance plans and testing schedules. Data exchanges with the FDIC and the FRB are expected to be Year 2000 compliant by October 31, 1998. If this compliance milestone is not met, the OCC will use bridge programs to ensure the continued proper execution of all data exchanges.

*Non-Mission-Critical IT Systems.* In our May report we identified 276 non-mission-critical IT systems, and indicated that 42 of those required renovation. As of August 14, 1998, the number increased to 307 non-mission-critical IT systems, due to the inclusion of 24 Lotus Notes applications developed since May and seven recently identified customer supported systems. Since our May report, the number of non-mission-critical IT systems requiring renovation also changed. As of August 14, 1998, 19 of our non-mission-critical IT systems require renovation, 27 will be replaced and 14 are to be retired. For those systems requiring renovation, eight have been renovated, and 11 are in process of renovation. We believe that the remaining 247 non-mission-critical IT systems, which do not require renovation, are Year 2000 compliant. All non-mission-critical systems are scheduled to be validated by September 30, 1998.

*Mission-Critical Non-IT Systems.* The OCC completed the assessment of mission-critical Non-IT systems on July 28, 1998, at our nine primary business sites. These nine primary sites are the Washington, DC Headquarters, the Landover, MD Data Center, the Houston, TX Ombudsman

Office, and the six District Offices. Mission-critical Non-IT systems are those systems which are located at the primary OCC sites and directly support the continuous operations of the building infrastructure as well as the life and safety of OCC personnel. As a result, their failure could affect OCC business continuity. Due to the critical importance of these systems, the OCC is working with the building management companies to facilitate the Awareness, Assessment, Renovation, Validation, and Implementation phases of the leased mission-critical Non-IT systems.

The OCC performed several tasks in completing the Awareness and Assessment phases. Initially, a Building Systems Survey Package was distributed to the building managers at the nine primary sites. The purpose of the survey was to raise awareness and begin to gather information regarding each site's mission-critical Non-IT systems. Next, the OCC conducted site visits. During the visits we delivered an awareness presentation and facilitated the development of an on-site inventory of the mission-critical Non-IT systems by the building management company. Following the site visits, the OCC facilitated the assessment of the mission-critical Non-IT systems by the building management companies with their vendors and manufacturers. We informed the building management companies about valuable tools and methodologies which assisted them in performing the assessments. As a result, they have been more willing to share information which has allowed us to accurately assess the business continuity risks associated with each primary site.

The OCC is now focusing its efforts on the Renovation, Validation and Implementation phases for the 29 mission-critical Non-IT systems located at the nine primary sites. Of the 29 systems identified, six or 21 percent are owned. The remaining 23 are leased. Eight of the 29 mission-critical Non-IT systems are non-compliant. The majority of these systems are Energy Management systems or Security systems. Of these, one has already been repaired, two are awaiting repair and five will be replaced. Following renovation, the repaired systems will be tested in the Validation phase prior to implementation. In addition to the non-compliant systems, equipment vendors or manufacturers verified that 17 mission-critical Non-IT systems at the nine primary sites are compliant. These systems will also be tested during the Validation phase. The remaining four mission critical Non-IT systems are undergoing assessment by building management companies in conjunction with their vendors and manufacturers. The OCC expects the building management companies to complete these assessments by October 31, 1998. Of the six Non-IT systems which are owned, five are compliant and one is in process of repair. We expect the one owned system to be renovated by September 30, 1998.

Building management companies at six primary sites plan to complete the Renovation, Validation and Implementation phases for their mission-critical Non-IT systems by March 31, 1999. Two sites reflect good progress but may not complete all phases by March 31, 1999, due to uncertainties in their testing plans and validation milestones. One primary site has made little substantive progress in the renovation, validation and implementation of mission-critical Non-IT systems. As a result, it is unclear if this site will complete all phases by March 31, 1999. The OCC plans to closely monitor the progress of the three primary sites which may have delayed

implementation. Our plan calls for continued follow-up, additional site visits and a review of our internal Business Continuity Plans. A review of our Bureau-wide Business Continuity Plan is necessary due to the uncertainties and the lack of formal recourse for ensuring that these mission-critical Non-IT systems are renovated, validated, and implemented in a timely manner.

*Non-Mission-Critical Non-IT Systems.* The OCC expects to complete the assessment of non-mission-critical Non-IT systems at 66 secondary office locations by March 31, 1999. We are projecting the renovation, validation, and implementation to be completed by September 1999, according to Treasury guidelines.

2. **Please report on the results of agency testing to date and the date by which the agency will have completed testing and implementation. Have there been any slippages with established test schedules? Please provide the status of business continuity and contingency planning for all mission critical systems and the full cost associated with implementing each plan. Please provide deadlines for completing these plans and testing them. Have trigger dates for implementing the plans been specified? If so, what are they? Please include in your explanation any accommodation in schedules for early fail dates of mission critical systems.**

*Testing.* The OCC set Year 2000 testing benchmarks for mainframe, client server, and PC applications. Each OCC system not scheduled for retirement or replacement must be tested to ensure Year 2000 compliance. Year 2000 test plans are customized for each application or group of applications. Date input, output, and database or file storage integrity must be verified. To be designated as Year 2000 compliant, a system must flawlessly process date and date-related data forward and backward across the Year 2000 boundary, and this result must be independently validated and verified. To facilitate testing procedures, the OCC created mainframe and client server test beds for application and implementation group testing. In addition, the OCC will use independent testing specialists who will assist application testers during the testing process. They will repeat the tests under a variety of conditions and document their findings.

Agency testing to date has been successful. Testing of renovated program code, especially the mission-critical systems, has proven the systems to be Year 2000 compliant, free of extraneous errors and in need of very little further revision. The systems and program code that the OCC implemented after Year 2000 renovation this past year performed normally and as expected in our production environment. The OCC is scheduled to complete the testing and implementation of all mission-critical IT systems, non-mission-critical IT systems, commercial-off-the-shelf (COTS) packages, and telecommunications equipment by October 31, 1998. The only slippages in test schedules were discussed in our response to Question 1.

*Contingency Planning.* The OCC developed contingency plans for all mission-critical as well as non-mission-critical systems and applications. Should renovation, validation, and implementation plans not proceed as planned, the OCC's contingency plans will help mitigate risks from a disruption of business functions. The contingency plans will also ensure continued business activity by the OCC and help reduce any negative impact on day-to-day operations.

The contingency plans for mission-critical systems include the following elements: a business impact assessment, a plan development outline, triggers for activating the contingency plans, and development and testing of contingency plans. Contingency plans for non-mission-critical systems follow the same methodology. However, the depth of the plans are dependent on the risks identified for each system.

The OCC also developed contingency plans for internal and external data exchange partners. In doing so, we spent considerable time evaluating our interfaces with other agencies, vendors, and customers. If the interface is internal, it will be renovated with a contingency plan developed to take into account the level of risk and dependence for the OCC partner(s). If the interface is external, the OCC will meet with the partners and adopt the most appropriate contingency plan.

All of our mission-critical systems have contingency plans that rely on manual intervention and either nonautomated or minimally automated processes. In the unlikely event that a mission-critical system fails because of a Year 2000-related problem, these processes will permit the OCC and its employees to continue to operate and fulfill their mission. Since these contingency plans depend so heavily on human resources, they are free from failure due to any ongoing Year 2000-related error and will be relatively inexpensive to implement, as we plan to use existing system and program administration personnel to staff these functions. All of the OCC's mission-critical IT system contingency plans will be tested in the first quarter of 1999. None of these systems have trigger dates prior to this time period. Please refer to Table 1.2 on page 3 for the mission-critical IT system schedule for specific system trigger dates.

3. **Please explain in detail the agency's plans for independently verifying compliance of repaired, replaced, and new systems. Include in the explanation the agency's methods (including configuration management methods) for ensuring that once systems are validated as compliant, any further changes to those systems (for regulatory or other reasons) do not result in such systems falling out of compliance.**

*Independent Validation and Verification.* This program will consist of a three-step process. First, OCC's application systems scheduled to be renovated will be reviewed and assessed by a team including contractors and OCC programmers. This renovation team will first modify necessary system components and then test the system for Year 2000 compliance. Second, after this team's work is complete, a separate test team of contractors and OCC personnel will independently validate and verify the systems' Year 2000 compliance. As a third check, an implementation team consisting of system user representatives will validate and confirm the operation of the system at the end of the implementation phase.

*Certification.* The final phase of OCC's Year 2000 compliance process is certification. Each phase of the Year 2000 compliance process creates documentation and an audit record of compliance activities. The OCC's certification process entails reviewing this documentation, conducting spot checks of systems to verify reported results, and interviewing participants to ensure process compliance. At the conclusion of this review, and based upon positive affirmation of Year 2000 compliance, an OCC Year 2000 Certification Form will be prepared and approved by both the system administrator and a representative of the Year 2000 Oversight Committee. This process establishes responsibility, accountability, and assurance that all planned compliance steps have been completed.

*Configuration Management.* Prior to the effort the OCC undertook to renovate, validate, and implement systems for Year 2000 compliancy, the agency had already established comprehensive application testing, configuration management, software migration and production control standards. These standards prescribe processes and rules that control and manage the flow of new and modified program code from the development environment to the production environment. All of the OCC's existing program code and systems have been or will be validated for Year 2000 compliance. All new systems now in development are designed and constructed to be Year 2000 compliant and will be subject to the same testing and certification criteria as code we are currently renovating. Program code and systems already certified as compliant, if changed, will be analyzed by the Year 2000 project team to determine what level of testing is required to retain Year 2000 certification.

## **INDUSTRY PROGRESS**

**Q1. Following the same format as last quarter, please provide an updated progress report for the quarter ending June 30, 1998, showing the Year 2000 status of all financial institutions under the agency's supervision. As before, please provide the numbers of institutions rated satisfactory, needing improvement, and unsatisfactory. For categories of institutions rated as unsatisfactory or needing improvement, please indicate the numbers of institutions in each category, their asset size, their location by state, the duration of the rating, and the nature and effectiveness of enforcement or other actions taken. Please indicate also whether institutions with less than satisfactory ratings last quarter are now rated satisfactory or visa versa.**

*Ratings Update.* Overall, the OCC believes national banks are making satisfactory progress in addressing Year 2000 problems. When we have found deficiencies we have worked with the institutions to correct them. Most of the deficiencies identified and corrected to date have related only to the first three phases of the remediation process. As institutions move into the testing and implementation phases, we anticipate that the problems they will face will be more challenging and more costly to resolve. Consequently, we anticipate that the summary ratings will fluctuate as institutions move through the testing and implementation stages, and as they continue to develop their contingency plans.

The following is a brief overview of Year 2000 summary evaluations for OCC-supervised institutions and common deficiencies for institutions that received less than satisfactory ratings.

- As of June 30, 1998, nearly 96 percent of institutions have a summary evaluation of satisfactory while four percent are rated needs improvement. Only eight institutions are rated unsatisfactory. In our first quarter results, 87 percent of national banks, federal branches and agencies, and independent data centers received satisfactory Year 2000 ratings, 13 percent received needs improvement ratings, and 17 institutions received unsatisfactory ratings. This change is partly attributable to banks' heightened awareness of Year 2000 issues resulting from FFIEC guidance and OCC monitoring.
- Based on our examinations to date, we have found that banks rated less than satisfactory demonstrated a number of common problems and deficiencies, including:
  - ▶ Incomplete processes to assess customer readiness.
  - ▶ Insufficient allocation of financial resources to complete necessary tasks.
  - ▶ Failure to meet scheduled deadlines.
  - ▶ Ineffective management oversight of Year 2000 efforts and reporting.

- Ineffective risk management process.

Table 1.1 summarizes the current distribution of Year 2000 summary ratings by asset size. The Year 2000 summary ratings do not vary substantially by region or state.

**Table 1.1**  
**Year 2000 Summary Evaluations**  
**By Asset Size**  
**June 30, 1998**

<i>Evaluation</i>	<i>&lt;\$100MM</i>	<i>\$100MM to \$500MM</i>	<i>\$500MM to \$1,000MM</i>	<i>Over \$1B</i>	<i>Overall Percent (# Banks)</i>
<i>Satisfactory</i>	95%	96%	97%	97%	96% (2,676)
<i>Needs Improvement</i>	4%	3%	3%	3%	4% (111)
<i>Unsatisfactory</i>	< 1%	< 1%	0%	0%	<1% (8)
<i>Number of Institutions</i>	1,563	900	134	198	2,795

*Source: OCC Year 2000 Database*

*Change in Ratings.* Ninety-seven percent of institutions to which the OCC examined and assigned ratings in the first quarter either have maintained or improved their Year 2000 summary ratings.

- Out of 368 institutions rated less than satisfactory at the end of the first quarter, 283 institutions (77 percent) received satisfactory ratings as of June 30, 1998.
- Out of 2,377 institutions rated satisfactory at the end of the first quarter, 32 institutions (one percent) received a less than satisfactory rating.
- Of the eight institutions rated unsatisfactory as of the second quarter, all are community banks with assets under \$500 million. At the end of the first quarter, two of these institutions were rated satisfactory, four were rated needs improvement, and two were rated unsatisfactory.

Table 1.2 provides a summary of the changes in summary ratings for institutions that migrated from a satisfactory rating in the first quarter to a less than satisfactory rating in the second quarter, and vice versa.

**Table 1.2**  
**Change in Year 2000 Summary Evaluations**  
**By Asset Size**  
**June 30, 1998**

<i>Change in Rating 3/31/98 to 6/30/98</i>	<i>&lt;\$100MM</i>	<i>\$100MM to \$500MM</i>	<i>\$500MM to \$1,000MM</i>	<i>Over \$1B</i>
<i>Satisfactory to Less than Satisfactory</i>	22	9	1	0
<i>Less than Satisfactory to Satisfactory</i>	163	80	13	27

Source: OCC Year 2000 Database

*Enforcement.* The OCC's enforcement policy is determined largely by: (1) the institution's Year 2000 summary evaluation; (2) progress made in complying with any previously issued supervisory directive or other informal or formal enforcement action; (3) the cooperation, responsiveness, and capability of the institution's management and board of directors; and (4) the time remaining prior to the Year 2000. For every institution that receives a needs improvement evaluation, the OCC sends senior management a Supervisory Directive detailing the specific Year 2000 deficiencies and setting forth specific measures to rectify the problem within specific time frames. The OCC takes more aggressive enforcement action when an institution receives an unsatisfactory Year 2000 summary rating.<sup>2</sup> The OCC initiates formal enforcement action whenever informal measures are inadequate or ineffective in securing prompt remediation of the Year 2000-related problems. There is a strong presumption that formal enforcement actions should be taken when informal remedial measures have been inadequate, ineffective, or otherwise unlikely to secure prompt correction of the institution's problems.

To date, the enforcement actions that the OCC has entered into appear to be effective in improving Year 2000 readiness. OCC examiners closely monitor banks' compliance with all OCC Year 2000 enforcement actions and will continue to monitor banks' progress as they enter the testing and implementation phases.

---

<sup>2</sup>On one occasion, the OCC initiated a formal enforcement action against a bank with a needs improvement summary rating.

Through August 26, 1998, the OCC has issued 274 Supervisory Directives.<sup>3</sup> Of the 274 Supervisory Directives, 124 were terminated after the institution made needed changes. As of August 25, we have issued four memorandums of understanding (MOUs). We also have issued one Commitment Letter. We have issued four Formal Agreements and one is pending. We have issued formal notices to three banks advising of our intent to issue a Safety and Soundness Order against them, and two of these banks are now operating under approved corrective action plans. In addition, we have entered a Consent Order with an independent data service provider that received an unsatisfactory Year 2000 summary evaluation.

---

<sup>3</sup>A Supervisory Directive is a written instruction from the OCC to bank management ordering the bank to take specific corrective actions necessary to effectively remediate a noted Year 2000 deficiency. It is considered an informal enforcement action. A Memorandum of Understanding is a two-party agreement between the OCC and the bank that is used to reflect the bank's commitment to correct its problems. It also is considered an informal enforcement action. A Formal Agreement is an agreement between the OCC and the bank that the OCC uses to require the bank's commitment to correct deficiencies and its violation can be used as the basis for a cease and desist order and result in the imposition of a civil money penalty (CMP). A Consent Order is a Cease and Desist Order issued with the consent of the institution. It is similar in content to a Formal Agreement but, in addition to the assessment of CMPs for violations, the order can be enforced through an action for injunctive relief in federal district court. A Safety and Soundness Order is similar in all aspects to a Consent Order, but it is imposed unilaterally by the agency following notice of failure to adhere to safety and soundness guidelines. Under 12 U.S.C. §1831p-1, the Federal banking agencies may require a bank that violates safety and soundness guidelines or regulations to file an acceptable plan. Further, if the bank fails to submit or implement a plan, the agency may issue a "safety and soundness order." To implement §1831p-1, the agencies issued in 1995 the "Interagency Guidelines Establishing Standards for Safety and Soundness." See 12 C.F.R. Part 30, Appendix A. The OCC believes that national banks that fail to implement an adequate Year 2000 remediation program violate these Guidelines and, accordingly, OCC has commenced actions under 12 U.S.C. 1831p-1 against such banks. The OCC and the other FFIEC agencies are exploring the further use of safety and guidelines. Formal Agreements, Consent Orders, and Safety and Soundness Orders are public documents; Supervisory Directives, Commitment Letters, and Memorandums of Understanding are not.

**Q2. Please outline the agency's plans for implementing the Year 2000 Phase II Workprogram for the second round of Year 2000 exams for financial institutions and service providers. Please explain how the agency will meet the more complex challenges of examining institutions' test results and contingency plans while at the same time facing a more compressed time frame of only about nine months to complete the second round. Include any staffing and other resource allocations or reallocations necessary to meet this need, as well as any assessments indicating that the agency may not have sufficient resources to complete the second round on schedule.**

*Year 2000 Supervisory Strategy.* The OCC's Year 2000 supervisory strategy is risk-based and "phase-focused." Specifically, it is designed to focus on where banks stand relative to the supervisory expectations for financial institutions during five key phases of a financial institution's Year 2000 project management process: awareness, assessment, renovation, validation, and implementation. During each of these phases, the OCC's goal is to ensure that the institutions it regulates and supervises are prepared to meet the challenges of the Year 2000 and that they do so in a manner that promotes a safe, sound and competitive national banking system.

As the banking industry begins to enter the most critical phase of its efforts to deal with the Year 2000 problem -- the testing phase -- the OCC and the FFIEC recognized that new examination procedures would be necessary to address the unique challenges that the testing and implementation phases will present. For many banks, testing will consume upwards of 60 percent of the cost and time spent to correct Year 2000 problems. The Phase II Workprogram was adopted by the FFIEC in June 1998 and is designed to be used through the first quarter of 2000.

The OCC's supervisory strategy calls for completion of two onsite examinations by June, 1999. The first, to be completed by year-end 1998, will focus primarily on banks' testing plans. This examination will ensure that each institution has an adequate test plan in place prior to commencing its testing program. The second, to be conducted in the first half of 1999, will assess testing results and contingency planning efforts. This examination will identify institutions that are experiencing difficulties completing their testing programs or have not developed sufficient contingency plans.

The planned timeframe for these examinations will enable the OCC to identify quickly those banks that experience testing problems. We expect there will be sufficient time available to correct any identified deficiencies in mission-critical systems prior to the Year 2000. We also believe there will be enough time for regulators to take corrective action should testing plans prove inadequate. OCC examiners will complete the FFIEC's Phase II Workprogram during these two examinations.<sup>4</sup>

---

<sup>4</sup>The objective of the Phase II examination procedures is to determine whether an institution is handling Year 2000 related issues in a safe and sound manner and whether the institution's Year 2000 testing plan meets the FFIEC's key milestones. These examination procedures focus mostly on the validation and implementation phases of the Year 2000 project plans and contingency planning.

The OCC also will continue to conduct more frequent Year 2000 on-site examinations in those banks with inadequate remediation programs. Additionally, OCC examiners will continue to conduct quarterly reviews at each national bank to update our information on their Year 2000 readiness.

*Industry Outreach.* To date, OCC representatives from the Washington headquarters office have participated in 54 outreach meetings with various groups, including bankers, service providers, software vendors and other representatives from the financial community. In conjunction with the other FFIEC agencies, we have held regular meetings to discuss Year 2000 issues with representative from the Bank Administration Institute (BAI), American Bankers Association (ABA), Independent Bankers Association of America (IBAA), and other financial institutions trade associations. Our six district offices have sponsored outreach programs with community, mid-sized, and credit card banks within each district. In addition to the OCC-sponsored district outreach meetings, district office management and staff have participated, or plan to participate in, approximately 90 outreach meetings around the country sponsored by the FFIEC and state bankers associations. To date, over 9,000 bankers have participated in meetings held in 38 states.

*Allocation of OCC Resources.* The OCC plans to allocate a significant portion of its supervisory efforts to ensure that the national banking industry is prepared to meet the challenges of the Year 2000. The OCC has significantly increased resources to address Year 2000 risks. Completion of Year 2000 supervision work has required, and is expected to continue to require, a redirection of some resources away from non-Year 2000 supervision activities. This has resulted in some delays in beginning regular on-site exams in small, highly rated, low-risk banks. However, we have not reduced our normal program of quarterly off-site reviews of all national banks during which we review the banks' current financial condition, update its risk profile, and revise our supervisory strategy as necessary to address any areas identified as having increasing risk.

Table 2.1 provides a quarterly overview of workdays and “full time equivalents” (FTEs) for our supervisory efforts through the first quarter of the Year 2000.

**Table 2.1**  
**OCC Year 2000 Supervisory Strategy**  
**Workdays and FTE Projections by Quarter**

<i>Activity</i>	<i>3Q98</i>	<i>4Q98</i>	<i>1Q99</i>	<i>2Q99</i>	<i>3Q99</i>	<i>4Q99</i>	<i>1Q00</i>
<b><i>Total Workdays</i></b>	<b><i>14,724</i></b>	<b><i>14,352</i></b>	<b><i>11,713</i></b>	<b><i>11,214</i></b>	<b><i>8,247</i></b>	<b><i>5,978</i></b>	<b><i>4,375</i></b>
<b><i>FTEs (Field and HQ)</i></b>	<b><i>92</i></b>	<b><i>90</i></b>	<b><i>73</i></b>	<b><i>70</i></b>	<b><i>52</i></b>	<b><i>37</i></b>	<b><i>27</i></b>
<b><i>Field FTEs</i></b>	<b><i>67</i></b>	<b><i>78</i></b>	<b><i>60</i></b>	<b><i>60</i></b>	<b><i>45</i></b>	<b><i>27</i></b>	<b><i>25</i></b>
<b><i>Field Employees*</i></b>	<b><i>268</i></b>	<b><i>312</i></b>	<b><i>240</i></b>	<b><i>240</i></b>	<b><i>180</i></b>	<b><i>108</i></b>	<b><i>100</i></b>

*Source: OCC Quarterly Year 2000 Supervision Plan*

\*One FTE equals 220 workdays or four people working full-time (55 days) during one quarter.

*Examination Support.* The OCC's Year 2000 supervisory strategy also includes a program to help our examiners address problems they encounter by providing them with support from technical experts, including OCC information technology staff and outside consultants.

- **Rapid Response Team.** The OCC has formed a rapid response team comprised of information technology (IT) and contracted experts to help examiners who request assistance on a particular examination. The team will be used to assess the impact of Year 2000 problems on the operations of banks that experience substantive testing problems or who are significantly behind FFIEC time deadlines.
- **Centralized Review of Data Centers.** During the month of September, a team comprised of examiners from the Bank Information System (BIS) cadre and Year 2000 consultants will review the testing plans of service providers and software vendors supervised by the OCC. This centralized review will provide consistent and timely review of testing plans that will help us identify key issues for the OCC to consider when assessing individual institutions' testing plans, and will facilitate follow-up supervisory activities for OCC examiners.
- **Training.** The OCC has an extensive and on going training program.
  - ▶ Nearly 600 OCC examiners have received advanced training on Year 2000 testing in July and August. The training program was developed by an FFIEC task force and was customized by a group of OCC BIS examiners to better address the

training needs of OCC examiners. We believe this group will provide a sufficient pool of examiners to meet our planned workday projections.

- ▶ We issued videos on the credit risk aspect of the Year 2000 for review at upcoming field staff meetings.
  - ▶ We are developing a CD-ROM-based training tool that all OCC employees can use on their personal computers to learn about the Year 2000 problem, FFIEC guidance, and the OCC's supervisory activities.
  - ▶ We plan to conduct a series of conference calls with OCC examiners conducting Year 2000 examinations over the next 12 months. The objective of these calls will be to inform the participants of the latest Year 2000 developments, answer questions, and address examination issues. The conference calls will be scheduled every four to six weeks, beginning in early September.
  - ▶ Additional training focusing on contingency planning and implementation will be developed in the fourth quarter 1998, with classes expected to be conducted in the first quarter 1999.
- Self Assessment Tool. In May, the OCC requested all national banks to complete a self-assessment form. The "Year 2000 Banker Self-Assessment" supplements the information gathered by OCC examiners. We are reviewing the results and plan to use them, together with information collected by examiners, to develop a Year 2000 screening model to help identify banks that exhibit high Year 2000 risk.
  - Year 2000 Help Desk. The OCC recently established a Year 2000 "help desk" to respond to questions examiners may have prior to completing Year 2000 examinations. Policy and operations staff, assisted by expert staff from our information technology services unit, will answer questions and assist examiners. OCC examiners can ask questions by sending emails and faxes to our Year 2000 policy unit. Answers to questions are posted on the OCC's internal Year 2000 webpage.

**Q3. Please provide an update progress report on the Year 2000 status of all service providers subject to the agency's supervision including the number rated satisfactory, needing improvement, and unsatisfactory. Please show for any service provider rated less than satisfactory the number of financial institutions dependent on its services and the degree of that dependence. Please indicate also whether service providers with less than satisfactory ratings last quarter are now rated satisfactory or vice versa. Please provide, where available, updated results of examinations of software vendors. Finally, please include some analysis of the degree to which service providers or software/hardware vendors are absorbing the costs of Year 2000 remediation or are shifting those costs to the financial institutions they serve.**

Nearly 70 percent of banks rely, in part or wholly, on service providers and software vendors for their mission-critical data processing needs. Therefore, ensuring that key service providers and software vendors provide Year 2000 ready goods and services to financial institutions is an important factor for reducing the likelihood of Year 2000 systemic risks.

In recognition of the role that third-party vendors play in processing data and developing software, the OCC and the other FFIEC agencies examine the largest service providers under the Multi-Regional Data Processing Servicers (MDPS) program and the largest software vendors under the Shared Application Software Review (SASR) program.

- There are 16 data centers and 12 bank software publishing companies that are in the MDPS and SASR programs, respectively. The OCC is the lead agency for 5 MDPS companies and 4 SASR companies. MDPS and SASR companies generally are national in scope.
- The OCC also supervises and examines 31 independent data centers (IDCs) used by national banks, which are regional in scope. In addition, the OCC examines 69 banks and affiliated servicers that provide data processing services to non-affiliated financial institutions.

Table 3.1 provides a summary of Year 2000 evaluations of OCC-supervised MDPS companies, SASR companies, independent data centers, and institutions that service non-affiliates.

**Table 3.1**  
**Year 2000 Summary Evaluations**  
**Service Providers and Software Vendors**  
**June 30, 1998**

<i>Summary Evaluation</i>	<i>OCC Supervised MDPS</i>	<i>OCC Supervised SASR</i>	<i>OCC Supervised Independent Data Centers</i>	<i>OCC Supervised Institutions serving Non-Affiliated Institutions</i>	<i>Total</i>
<i>Satisfactory</i>	<i>5</i>	<i>4</i>	<i>28</i>	<i>67</i>	<i>104</i>
<i>Needs Improvement</i>	<i>0</i>	<i>0</i>	<i>2</i>	<i>2</i>	<i>4</i>
<i>Unsatisfactory</i>	<i>0</i>	<i>0</i>	<i>1</i>	<i>0</i>	<i>1</i>
<i>Total</i>	<i>5</i>	<i>4</i>	<i>31</i>	<i>69</i>	<i>109</i>

*Source: OCC Year 2000 Database*

*Update on Year 2000 Evaluations.* As of June 30, five out of 109 OCC-supervised service providers and software vendors have received less than satisfactory ratings. Four have received needs improvement ratings and one has received an unsatisfactory rating. The OCC issued a Supervisory Directive for each service provider that received a less than satisfactory rating. The servicer that received an unsatisfactory rating provided data processing services to 15 financial institutions. The OCC worked closely and cooperatively with that servicer, other FFIEC agencies, and the customers of the servicer to ensure that it took corrective action. In response to our timely supervisory action, the servicer is taking appropriate steps to address deficiencies noted by the OCC.

*Change in Ratings.* The summary rating for nine service providers (out of 10) increased to satisfactory ratings from less than satisfactory ratings. Ratings for four institutions dropped from a satisfactory rating as of March 31, 1998 to a less than satisfactory rating by June 30, 1998.

The five data centers that received less than satisfactory ratings as of June 30, 1998 provide services to 27 financial institutions. Table 3.2 provides an overview of the ratings and the number of client institutions.

**Table 3.2**  
**Number of Client Institutions for**  
**Service Providers and Software Vendors**  
**with Less than Satisfactory Ratings**  
**June 30, 1998**

<i># of Institutions</i>	<i>Rating</i>	<i>Client Institutions</i>
<i>4</i>	<i>Needs Improvement</i>	<i>12</i>
<i>1</i>	<i>Unsatisfactory</i>	<i>15</i>
<i>Total</i>		<i>27</i>

*Source: OCC Year 2000 Database*

*Cost Allocation Practices.* Service providers and software vendors absorb and allocate their Year 2000 remediation costs in different ways. Some recover costs through existing charges by requiring client financial institutions to upgrade to compliant systems or charging special fees to conduct Year 2000 testing.

**Q4. Please provide a summary of any Year 2000 findings and recommendations of the agency's Inspector General and how the agency has responded to each.**

The Treasury Inspector General has not fully completed its review of the OCC's Year 2000 efforts. That review started in mid-April of this year, with field work beginning in May. The person in charge of the review has informed us that the field work is scheduled to be complete by the end of August and that we should not expect a report until after the end of September. Once we receive that report, we can provide the committee a summary of findings and recommendations, as well as a discussion of proposed agency responses.

**Q5. In the area of credit risk, please provide a status report on the number of institutions which successfully met the FFIEC deadline of June 30, 1998, by which institutions were to have in place a due diligence process to control Y2K risks posed by customers. To the extent possible, please report on the progress of financial institutions toward meeting the next September 30, 1998, deadline for banks to assess individual customer's Y2K preparedness. Finally, please address how the current effort at identifying Y2K credit risk is impacting asset quality ratings for institutions.**

*Status.* As of June 30, 1998, OCC's Year 2000 reporting system reveals that 107 (about four percent) of OCC supervised institutions would not meet the June 30, 1998 deadline by which institutions were to have in place a due diligence process to control Year 2000 risks posed by customers. Our examiners are reviewing bank compliance with this requirement during the third quarter and will be able to confirm in October whether their institutions did, in fact, put in place adequate controls to address credit risk. To date, our examinations reveal that most large banks have implemented Year 2000 credit risk management controls, but the sophistication of those controls differs widely. Our examinations reveal that many community banks have a general awareness of this issue, but are not as far along as large banks.

We are working closely with national banks to ensure that they understand the importance of establishing a due diligence process to assess and control credit risk issues associated with Year 2000-related operational failures. As part of our industry outreach efforts, we discuss the FFIEC Year 2000 customer risk concerns.

*Shared National Credit Survey.* During the recent shared national credit review conducted in the second quarter of 1998, the OCC surveyed 45 large national banks and federal branches and agencies to determine the status of their efforts to comply with the credit risk aspects of the FFIEC guidance on customer risk. The shared national credit review covers a significant portion of loans provided by the banking system. Our survey was structured to identify the current status of individual bank efforts, common practices, and to determine whether process and procedural deadlines included in the guidance would be met. The survey results provided more insight into the large bank population's efforts to assess and manage the risk posed by its credit customers' Year 2000 preparations.

The survey reveals the following:

- Eighty percent of banks in the survey have a process in place to evaluate customer preparedness for Year 2000.
- All banks in the survey expect to complete the assessment of customer preparedness and categorize the risk as being low, medium, or high by the September 30 deadline.
- The most common criteria for identifying material customers is size of the relationship. The next most frequently used determinant is the customer's reliance on technology.

- The most frequently mentioned controls include covenants on adequate resources to achieve Year 2000 compliance, increased reserves to the ALL, reduced credit lines, and shortened credit maturities. Other practices include providing loan officers with sufficient training to perform a basic assessment of Year 2000 customer risk and requiring officers to determine if Year 2000 credit risk primarily impacts the customer's cash flows, balance sheet, or supporting collateral.

*Credit Challenges.* Based on examination results to date, our work in large national banks, and the shared national credit survey, we believe that most banks will meet the September 30, 1998 deadline. There are, however, several challenges facing national banks.

- Credit markets are sufficiently liquid that borrowers can readily obtain funding without Year 2000 restrictions. To preserve long established relationships with important customers, many national banks have decided to rely on existing covenants, rather than adding Year 2000-specific provisions. When some banks have attempted to write Year 2000 language into loan agreements, customers, up until recently, resisted.
- Banks are experiencing difficulty in their efforts to integrate Year 2000 assessments of customers into their risk rating systems. Presently, most banks view Year 2000 as one additional credit factor to be considered along with the other more traditional factors. We expect that the methodologies banks use to integrate Year 2000 assessments into the risk rating process will vary depending on the technological dependence, the capacity of borrowers to successfully address Year 2000 concerns, collateral, etc. As a result, banks' Year 2000 assessments have not yet had a significant impact on asset quality ratings.
- Examiners report banks are finding the results from surveys they have sent to their borrowers asking for information on the Year 2000 risk are of limited value due to poor data quality. Many banks now are conducting face-to-face meetings with borrowers and sharing Year 2000 information on the banks' efforts in order to obtain Year 2000 information on their borrowers.

**Q6. As a follow-up to last quarter's reports, please provide a progress report on the success of financial institutions in obtaining Year 2000 readiness data from local utilities and telecommunications providers. In this regard, please include in your answer an assessment as to whether the President's proposed "good Samaritan" legislation, relating to Year 2000 disclosures, would facilitate the kinds of disclosures financial institutions need from third parties such as utilities or telecommunications companies or facilitate the sharing of Year 2000 information among financial institutions themselves.**

*Telecommunications/Power Companies.* During the first quarter, many banks expressed concerns that telecommunications and power companies were not disclosing adequate information on their Year 2000 remediation efforts. In response, the OCC and the other FFIEC agencies began meeting with government officials to discuss infrastructure concerns. We continue to participate in the President's Council on Year 2000 Conversion and have urged telecommunications and power companies to share information on the readiness of these critical industries.

Over the past quarter, national banks and federal branches and agencies have received more information on the Year 2000 readiness efforts of telecommunications providers and power companies. Many national banks and federal branches and agencies report that their telecommunications providers are making adequate progress towards remediating and testing telecommunications networks. Less information has been forthcoming from power companies.

The OCC is concerned that many infrastructure-related companies will not be ready for external testing until well into 1999. For some, we understand that testing with customers may not begin until the second or third quarter of 1999. This increases the risks to the banking system and reduces the time to react to problems, should these utility companies' remediation efforts encounter any problems which further delay external testing. OCC assessments of bank testing results will be tempered by these circumstances, and may not adversely affect the ratings of national banks if they have made good faith efforts to test with all material customers and third parties.

The OCC continues to remind national banks and federal branches and agencies to gather information and assess Year 2000 readiness efforts of all mission-critical service providers, including telecommunications providers and power companies. OCC examiners will review progress as part of the Phase II Workprogram that all examiners are using at this time.

*"Good Samaritan" Bill.* The Administration's Year 2000 disclosure bill, the "Good Samaritan" bill (H.R. 4355 and S. 2392) is intended to encourage the disclosure and exchange of information on Year 2000 issues. Under the bill, in order to recover in a civil suit based on an allegedly false or misleading Year 2000 statement, a claimant must establish certain specific elements, including knowledge that the statement was false, inaccurate, or misleading and that there was an intent to mislead or deceive. The OCC believes that this legislation will encourage voluntary disclosure and a meaningful exchange of information on Year 2000 remediation activities, such as information exchanges among power and telecommunications companies and the financial

institutions they serve.

**Q7. Please provide the agency's latest assessment of the systemic Y2K risk to the nation's banking and financial services industry, including in particular the potential liabilities for the insurance funds. Please describe the latest developments (at the agency or interagency level) in industry-wide testing and contingency planning for the Year 2000. Include in your response any policy deliberations on, or trigger dates establishing for, regulatory agency takeovers of institutions (or actions against service providers) that are not going to be compliant on time.**

The OCC's assessment of the systemic Year 2000 risk to the nation's banking and financial service industry has not changed substantially since our May 14 report. At this stage in the remediation process, we believe that it is too early to estimate potential liabilities for the insurance funds. During the coming months, as institutions begin testing their systems, we will be better able to assess the principal risks to the industry. The OCC is working closely with the FDIC to analyze potential risks to the deposit insurance funds. The following is a brief overview of the significant strategic issues facing the banking and financial services industry and our ongoing plans for addressing these concerns.

*Testing.* Testing is critical to ensure that remediation efforts work effectively. The FFIEC agencies issued guidance on testing in April, provided updates to that guidance in the recently issued "Questions and Answers Concerning FFIEC Year 2000 Policy," and are focused on testing in the Phase II examination procedures. In addition, the OCC and the other FFIEC agencies are participating in industry-sponsored conferences and seminars to emphasize the importance of testing and to answer questions regarding FFIEC expectations. We are working closely with the Bank Administration Institute (BAI) regarding their efforts to conduct bank-to-bank and bank-to-counterparty testing. Also, the OCC and the other FFIEC agencies are monitoring the efforts of the Mortgage Bankers Association to coordinate testing of mortgage banks and mortgage-related government sponsored enterprises (GSEs).

The OCC and the other FFIEC agencies continue to support efforts of the bank trade associations to coordinate testing efforts more broadly within the financial services industry. As well, the Federal Reserve (Fed) is participating in key industry testing of clearing and settlement processes with other settlement providers. In addition, the major settlement and clearing system providers, including the National Automated Clearinghouse Association (NACHA), New York Clearing House Association (NYCHA), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT), have scheduled tests with financial institution customers.

*Contingency Planning.* The OCC is involved in several significant contingency planning efforts. First, the OCC has participated in an interagency working group, including representatives of the Federal Deposit Insurance Corporation (FDIC), the Fed, and the Office of Thrift Supervision (OTS), to determine what conditions must exist for a financial institution that fails to remediate its Year 2000 problems to be declared insolvent, thereby triggering the appointment of a receiver. The findings of the group yielded information that will be useful in the identification of institutions

with significant potential to fail because of Year 2000 problems and that will be the foundation for more targeted interagency contingency planning in the future.

Second, the OCC is developing contingency plans to deal with the industry's capacity to absorb non-Year 2000 ready institutions. During upcoming examinations of bank data centers and non-bank service providers, the OCC will be querying and capturing information on the data centers' and service providers' capacity to service new clients due to Year 2000 problems. The OCC and the other FFIEC agencies are beginning to compile a "bidders list" for Year 2000 purposes that will include institutions that have a demonstrated, well managed Year 2000 program and that has the capability to process acquisitions of other institutions.

Third, the OCC established an internal working group to develop regulatory options for addressing bank-specific and systemic risk concerns. As part of this effort, the OCC is developing plans to deal with local problems that might temporarily disable banks in particular areas (e.g., the failure of a local utility or telephone company). The group now is prioritizing these concerns and assigning responsibility to develop contingency plans to address what banks and regulators need to do.

Fourth, the OCC is developing contingency plans for events that may arise from Year 2000 problems in individual national banks, such as a bank's failure to complete the remediation phase of mission-critical systems or its business resumption plan.

Fifth, the OCC's legal staff is finalizing a review of our legal authority to close banks due to Year 2000 failures.

*Public Confidence.* Educating bank customers about the Year 2000 problem is critical to minimizing unnecessary public alarm, which could cause serious problems for financial institutions and their customers. The OCC and the other FFIEC agencies have issued guidance instructing financial institutions to provide complete and accurate responses to questions and concerns raised by their customers. The OCC has asked each national bank to develop a customer awareness program by September 30, 1998. This program should include appropriate communications channels to effectively respond to customer inquiries. The program also should address how the bank will respond to its customers should unfavorable events occur, whether those events are caused by internal bank problems (e.g., system breakdown) or external (e.g., adverse media coverage of Year 2000, computer problems elsewhere). The OCC and FFIEC will continue to consider further efforts to encourage banks to educate their customers about the Year 2000 problem.

*Conversions.* Service providers estimate it will take upwards of three to six months for small-to-medium size institutions to convert to new service providers in the event their provider will not be prepared for the Year 2000, and 12 to 18 months for large complex institutions to convert. In addition, institutions that need to convert to other service providers or software providers may find that the companies that have the capacity today may not have the capacity in mid-to-late

1999. During the upcoming examinations of service providers and software vendors, the OCC plans to gather information on the industry's capacity to absorb non-compliant institutions. The OCC also plans to develop appropriate contingency plans to address these issues with the other regulators. Two critical questions that will need to be answered in this regard are: (1) how many institutions may need to convert to new providers, and (2) how long can they wait to make the conversion? Although whether an institution converts to a new system in 1999 is a decision for the institution's board of directors, the OCC will assess the risk resulting from such a conversion on a case-by-case basis.

*Mergers and Acquisitions.* Year 2000 readiness is clearly an important factor to consider in any merger and acquisition that takes place during the next 16 months. For example, some banks may seek to be acquired by institutions with more advanced technology and Year 2000-ready systems as a way to preserve shareholder value and avoid operational failures. For mergers involving complementary product lines or non-overlapping geographic markets, full-scale systems integration may be delayed until after January 1, 2000, to ensure that information technology resources are not diverted from existing Year 2000 projects. Full-scale systems integrations involving similarly-sized, large institutions will become increasingly difficult to complete as we get closer to January 1, 2000, particularly if one of the merging banks is behind schedule in implementing its Year 2000 project plan.

The OCC is currently evaluating whether, and if so how best, to strengthen an advisory we sent to national banks in January 1998 regarding Year 2000 considerations in corporate applications.

**Q8. Please provide the agency's latest assessment of the Year 2000 status of the international banking and financial services sector. Please describe what steps the agency is taking in such areas as testing with foreign institutions and payment systems and contingency planning, to protect the US financial system from such risks.**

*International Year 2000 Status.* Based on information obtained from our internationally active national banks as well as through external outreach activities, we see some positive signs that Year 2000 awareness and action is increasing around the world. We have seen increasing evidence of Year 2000 awareness in that attendance at international working group meetings has increased and participants demonstrate greater understanding of the risks. Unfortunately, some countries are just now beginning to initiate Year 2000 awareness programs encompassing their financial markets, clearing and settlement systems, and important infrastructure platforms.

- Attempts by U.S. bankers to analyze Year 2000 status in foreign countries are confronted by several challenges. First, many developing countries are preoccupied with economic turmoil and thus are unable to focus adequately on the problem. These same countries often do not have public and private sector organizations that could provide the market with reliable information on their Year 2000 efforts. Second, some developed countries have stated publicly that the Year 2000 problem is not a serious issue, further alarming bankers who recognize, based on first-hand experience, that the Year 2000 risks in those countries are significant. Third, we are concerned that the attention being directed to reprogramming in connection with the introduction of the Euro may be distracting countries from addressing the Year 2000 issue.
- Current Year 2000 information on some countries' efforts is incomplete, making it difficult to make qualitative judgments as to their level of preparedness. The OCC is concerned that any lack of Year 2000 "hard" information from countries or their key markets will increase the importance of the "market perception" of Year 2000 risk in these countries. Even countries that have made good progress in dealing with the Year 2000 challenge need to make markets aware of their efforts or they will potentially suffer from the perception that they are not dealing with their problems. Computer problems that focus public attention on the Year 2000 problem could create the perception of serious Year 2000 difficulties in lagging countries, and trigger a negative market reaction before the year 2000 arrives. Such triggers might be associated with computer systems failures linked to the introduction of the Euro on January 1, 1999, or to the so-called computer reset date, September 9, 1999. Possible overreaction by market participants and the general public to their perceptions of global Year 2000 risk also could precipitate instability in the global financial markets, including those attributable to global Year 2000 risk.
- Through the efforts of several global Year 2000 multilateral groups, particularly the

Global 2000 Coordinating Group<sup>5</sup> and the Joint Year 2000 Council, unprecedented international collaborative initiatives are underway to identify areas where cross-border coordination could facilitate efforts by the global financial community to improve global Year 2000 readiness of trading, settlement and payment systems; to coordinate testing schedules in key financial markets; to discuss possible contingency measures; and to establish linkages with international public and private sector Year 2000 programs.

- OCC examiners assigned to our largest and most internationally active national banks are reporting that these institutions are working diligently, as FFIEC guidance directs, to develop appropriate contingency plans to mitigate risks to those foreign agencies, customers and counterparties that are not testing their Year 2000 readiness thoroughly or successfully. The full extent and timing of U.S. banks' contingency plans for global Year 2000 risk is not yet defined, but the next phase of our Year 2000 examination program will focus on banks' efforts to develop appropriate contingency plans for potential problems arising from Year 2000 induced failures.

*OCC International Year 2000 Activities.* In light of the potential seriousness of any major market disruptions caused by real or perceived Year 2000 concerns, the OCC has taken several specific steps to gain better insight into market perceptions of global Year 2000 readiness, assess the state of readiness of foreign financial markets, and monitor Year 2000 contingency planning efforts of national banks.

- The OCC is actively collecting global Year 2000 readiness information through our examination process as well as through extensive external outreach activities with market participants and domestic and foreign financial industry regulators. The OCC has established a Global Banking Coordinator's office staffed by full-time senior large-bank examiners with responsibility for researching and maintaining data on Year 2000 risk in foreign countries and assessing market perceptions of risk and potential market reactions. This unit is building a Global Year 2000 Risk Analysis database to support our supervisory efforts and will help the OCC identify potential problem areas as well as market perceptions regarding global Year 2000 readiness that could have an impact on the U.S. banking system. The database will include regional and country specific information on foreign public- and private-sector Year 2000 preparations and will help the OCC identify and assess consensus market perceptions regarding the Year 2000 progress of key foreign governments, financial systems, clearing and settlement systems, and infrastructure that could have an impact on the operations of U.S. banks.

---

<sup>5</sup> The Global 2000 Coordinating Group includes representatives from financial services firms that are located in and operate across multiple markets (including banking, securities and insurance markets) and jurisdictions. The group is hosted by the Swiss Bank Corporation, and it currently consists of 77 institutions and associations representing 18 countries. The U.S. Steering Committee members are Bankers Trust, Citibank, Chase, J.P. Morgan, Lehman Brothers, Merrill Lynch, Morgan Stanley Dean Witter, Salomon Smith Barney, and the Securities Industry Association.

- The OCC is working with the Global 2000 Coordinating Group in its efforts to identify multilateral outreach strategies for foreign Year 2000 risks and appropriate contingency action plans that would mitigate the risk arising from inadequate Year 2000 preparations by foreign market participants. The Global 2000 Coordinating Group is in the process of collecting self-assessments on Year 2000 readiness information from countries where national banks have significant relationships and discussing global Year 2000 testing and contingency planning issues. This information will prove valuable to the assessment of the risks that global Year 2000 disruptions may pose to the U.S. banking system.
- The OCC also is actively participating in the Basle Committee's Year 2000 Task Force and liaising with the Joint Year 2000 Council. Through these multilateral groups of international financial market regulatory authorities, the OCC is working with foreign bank supervisors to encourage more information sharing on regulatory Year 2000 strategies, discussing possible contingency measures, establishing linkages with national and international private sector initiatives, and promoting more aggressive international Year 2000 remedial action.

**Q9. Please advise the Committees if the agency anticipates a need for new legislation, particularly as it may relate to ensuring Year 2000 compliance at financial institutions or in implementing business continuity or contingency plans at the agency or at financial institutions. Also, please advise the Committees if the agency contemplates taking any action of a regulatory nature which relates to increasing or decreasing non-Y2K related information technology obligations of financial institutions.**

*Legislation.* The OCC believes that the Bank Service Company Act (BSCA) should be amended to clarify that, under current law, entities providing services to banks under contract or otherwise are subject to enforcement actions with respect to the performance of those services. Such an amendment would clarify that the appropriate Federal banking agency that has examination authority for a bank, or a subsidiary or affiliate of that bank also has the authority under the BSCA to bring an enforcement action under 12 U.S.C. § 1818 against the entity that is providing services under contract or otherwise to the bank or its subsidiary or affiliate.

Banks increasingly are relying on service providers to provide data processing and other important services that are essential for the safe and sound operation of the institution. For example, service providers may provide services to banks and their subsidiaries and affiliates that will determine whether that entity is Year 2000 compliant. The amendment will clarify the banking agencies' authority under current law to bring enforcement actions against a service provider with respect to the performance of such services if, for example, the services being provided may cause the bank to be Year 2000 non-compliant or constitute unsafe or unsound banking practices. The appropriate Federal banking agency's ability to bring such an action could encourage a service provider to take the necessary actions to achieve Year 2000 readiness.

The Examination Parity and Year 2000 Readiness for Financial Institutions Act, enacted earlier this year gave the OTS and NCUA authority to take enforcement action against service providers, designed to parallel the current authority of the banking agencies under the BSCA. Because of the different format and terminology used in that Act, however, the OCC believes language is necessary to clarify that all the banking agencies have comparable authority to take such actions on an ongoing basis. We have attached draft legislative language for the Committees' consideration.

*Regulatory Actions.* In February 1998, the OCC issued guidance on risks associated with banks' use of technology. The Technology Risk Management Bulletin (OCC 98-3) describes the primary risks related to banks' use of technology and a risk management process for how a bank should manage these risks. On August 26, 1998 the OCC issued guidance to bankers and examiners on how to identify, measure, and control risks arising from the use of retail PC banking. "Technology Risk Management: PC Banking" defines risks and supervisory concerns regarding proprietary network and Internet banking systems. The bulletin responds to the growth in the availability and use of retail electronic delivery systems by banks. Many of the issues discussed in the bulletin also are relevant with respect to other electronic banking technologies, including

telephone banking, “kiosk banking,” and palmtop computers.

Later this year, the OCC will issue guidance on risks in electronic authentication, including digital signatures and certification activities. This technology is still in the early stages of market development; however, banks are expected to play an important role as certification authorities. A “certification authority” is a trusted third party that confirms the identities of parties sending and receiving electronic payments or other communications. This service is referred to as electronic authentication. The electronic authentication guidance will provide basic information about this technology and identify the primary risks for national banks that are considering investing in or operating a certification authority system.

Attachment

**Clarification of Enforcement Authority  
Over Service Providers  
Under the Bank Service Company Act**

Section 7(c)(1) of the Bank Service Company Act (12 U.S.C. 1867(c)(1)) is amended by striking “regulation and examination by such agency” and inserting “regulation, examination, and enforcement under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818) by the appropriate Federal banking agency”.

As amended above, the statute would read--

“(1) such performance shall be subject to regulation, examination, and enforcement under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818) by the appropriate Federal banking agency to the same extent as if such services were being performed by the bank itself on its own premises, and”.

**Explanation:** This language amends the section 7c of the Bank Service Company Act (BSCA) to clarify that service providers that are providing services to banks under contract or otherwise may be subject to enforcement actions with respect to the performance of those services. It clarifies that the appropriate Federal banking agency that has examination authority for a bank, or a subsidiary or affiliate of that bank, also has the authority under the BSCA to bring an enforcement action under 12 U.S.C. § 1818 against the service provider that is providing services under contract or otherwise to the bank or its subsidiary or affiliate. The appropriate Federal banking agency may bring an enforcement action against the service provider in the same manner that it could bring an enforcement action against the bank itself if the services were performed on the bank’s own premises. Under the BSCA, the banking agencies have the authority to issue any regulations and orders that are necessary to carry out this law.

This amendment is needed to clarify that the appropriate Federal banking agencies have the authority to bring actions against companies that are providing services to banks or their subsidiaries or affiliates that may result in an unsafe or unsound condition or a violation of law or regulation. Banks are increasingly relying on service providers to provide data processing and other important services that are essential for the safe and sound operation of the institution. For example, service providers may provide services to banks and their subsidiaries and affiliates that will determine whether that entity is Year 2000 compliant. This amendment will clarify that the banking agencies have the authority to bring enforcement actions against a service provider with the respect to the performance of such services if the services will cause Year 2000 noncompliance or any other unsafe or unsound condition. The ability of banks to bring such an action could encourage a service provider to take the necessary actions to achieve Year 2000 readiness.